UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA, v. ROMAN STORM, et al., Defendants.	Case No. 23 Cr. 430 (KPF)

BRIEF OF AMICUS CURIAE COIN CENTER IN SUPPORT OF DEFENDANT ROMAN STORM'S MOTION TO DISMISS

Peter Van Valkenburgh*
Coin Center
700 K St. NW
Washington, D.C. 20001
peter@coincenter.org

**pro hac vice applications forthcoming*

Cameron T. Norris*
Daniel M. Vitagliano (SDNY 5856703)**
Jeffrey S. Hetzel*
Consovoy McCarthy PLLC
1600 Wilson Boulevard, Suite 700
Arlington, Virginia 22209
(703) 243-9423
dvitagliano@consovoymccarthy.com

*** supervised by principals of the firm admitted to practice in Virginia*

Counsel for Amicus Curiae Coin Center

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE

Coin Center is a Washington, DC-based non-profit research and advocacy center focused on the public policy issues facing cryptocurrency and decentralized computing technologies such as Bitcoin and Ethereum. Our mission is to defend the rights of individuals to build and use free and open cryptocurrency networks: the right to write and publish code – to read and to run it. The right to assemble into peer-to-peer networks. And the right to do all this privately. Coin Center is separately suing OFAC to remove the Tornado Cash pool addresses from the SDN list. Coin Center is arguing that OFAC's action exceeds its statutory authority by blocking things like immutable smart contracts that are neither sanctioned persons nor their property, violates the Administrative Procedure Act, and is unconstitutional. *See Coin Center et al. v. Secretary, Dep't of Treasury, et al.*, Case No. 23-13698-E (11th Cir.). While the issues in our case and this case relate to common underlying facts, the legal issues are different and the outcome in this case would not be determinative in ours.[1]

ARGUMENT

The prosecution's indictment betrays a fundamental misunderstanding of how the Tornado Cash privacy protocol works and what role the developers of that protocol have in its use and operation. To assist the court, we will begin with a detailed description of how the protocol and the underlying Ethereum protocol works and to what degree any third party, including the Defendants, has power or control over funds moved by that protocol. In light of this more detailed understanding of the protocol, we will argue that the actions of the Defendants cannot give rise to sanctions liability under the relevant standards in the International Emergency Economic Powers Act (IEEPA) and the associated "Berman Amendment" carve-outs for transactions in information. Finally we will argue

[1] The government and Mr. Storm consented to the filing of this brief. No party authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund preparing or submitting the brief; and no person—other than amicus curiae, its members, or its counsel—contributed money that was intended to fund preparing or submitting the brief. *See* Fed. R. App. P. 29(a)(4)(E).

that even if these statutory arguments failed, the actions of the Defendants are characterized as "pure speech" under relevant First Amendment case law, and that the prosecution's aggressive application of IEEPA through conspiracy charges is not narrowly tailored to achieve a compelling government interest.

I. Technical Background on Ethereum

Ethereum is a network of computers on the internet. The computers collectively work together to create a shared public database of user data, including personal financial transactions. That database is typically referred to as Ethereum's "blockchain," a term of art referencing the specific technological methods used to encode and verify the data in the database. Ethereum is used by tens of millions of Americans. It facilitates transactions involving ether, the second most common cryptocurrency in America. It also facilitates transactions involving a wide range of additional crypto assets often referred to generally as "tokens." To use Ethereum, a person need only have an internet-connected device and freely available software. That software is "free and open-source" which means it is free as in gratis, *i.e.* it is available for users to download from a multitude of sources without any cost. It is also free as in freedom, *i.e.* it is released under open-source copyright licenses that allow anyone to use, modify, distribute, and copy it without permission and as they see fit.

Using this free software on her own computer, a person can begin transacting on Ethereum. As a first step she must have her computer generate an Ethereum address and a corresponding "private key." The address is a random but unique number that will represent the user on the Ethereum network. The private key allows her to digitally sign messages such that everyone else on the network can verify that the sender of the message is the person who created the address rather than an imposter. By sharing an address, users are able to receive tokens from anyone, anywhere in the world. Unlike a traditional payment service, sending and receiving tokens on Ethereum does not require an intermediary. Instead, the sender broadcasts their intent to transfer tokens, digitally signs

their message using the corresponding private key, and Ethereum's network collectively updates the blockchain records of the sender and receiver addresses with the new balances.

In addition to sending and receiving tokens, users can create and interact with "smart contracts," which are software tools that extend the functionality of Ethereum. When software developers program smart contracts, they decide what operations the smart contract will support and what rules those operations must follow. These rules and operations are written using code that is broadcast to Ethereum's network, just like the token transactions described above. Once a smart contract's code is added to Ethereum's records, it receives a unique address and can be interacted with by any user to automatically carry out the rules and operations it supports. Both people and smart contracts can have Ethereum addresses. The difference is that when a person has an address they have the private key that controls any tokens sent to that address. That person will ultimately decide if and when any transactions are made with those tokens. When a smart contract has an address, the rules and operations written in the smart contract code control the tokens. They could be simple rules – such as "automatically return the tokens to the sender" – or more complicated rules. There could be rules that include human operations and human decisions – such as "send the tokens back if 3 out of 5 of these human-controlled addresses send a signed message saying they agree." The rules could also, however, be fully and permanently outside of any human being's control. In that case, so too are any tokens sent to that address until and unless the contract sends them to some human according to the rules. When a smart contract's rules are programmed to operate without human involvement, the contract is often referred to as being "non-custodial," as in no human participant custodies any assets on behalf of the users of the contract.

By default, smart contracts are "immutable," which means they cannot be removed or modified (updated) by anyone once they are "deployed," a term of art for publishing the code to the Ethereum blockchain. Smart contracts can alternatively be deployed with an update capability assigned

to some human-controlled address. Update capability can also be subsequently revoked. Revocation also creates an immutable contract; the code and its attendant functionality will persist on the ethereum blockchain irrespective of the actions of the original developers or any other person.[2]

Unlike traditional finance, Ethereum's records are completely transparent: anyone can download and view the balances and transaction history of its user accounts. Although user addresses are pseudonymous, if a real-world identity is linked to a user address, it becomes possible to trace that user's complete financial history. By default, a record of a casual transaction today, like paying cryptocurrency for Wi-Fi access at the airport, leads directly to records of earlier cryptocurrency transactions, which may include any intimate, revealing, or sensitive transactions made by the same user long ago. Among the many different applications smart contracts may support, they may also provide an avenue for users to regain the privacy they expect when interacting with financial systems.

II. Technical Background on Tornado Cash

The Tornado Cash protocol is a series of smart contracts and off-chain software tools that allow users of Ethereum to protect their privacy when transacting despite the inherent public visibility of transactions on Ethereum's blockchain. It is to Ethereum users what a set of drapes would be to someone with large picture windows in their bedroom. All of the Tornado Cash smart contracts that receive user assets, the "pool" addresses, have been deployed to the Ethereum blockchain such that they are both non-custodial and immutable. Therefore, when a user sends assets to these addresses,

[2] To revoke update capability, the person or group of persons who currently have the power to update the contract must transfer that update permission to a placeholder Ethereum address for which it is mathematically infeasible to derive a private key. All the computing power in the world could be dedicated exclusively to creating a corresponding private key for the next billion years and yet still no computer would likely succeed at creating that matching key. Without a corresponding private key it is impossible for any person to forge a correct digital signature updating the contract. This placeholder address is known as "the zero address." Once the ability to update a contract has been assigned to the zero address it is, effectively revoked, it cannot be reclaimed and the contract can no longer be changed.

the user and the user alone is in control of her assets; no third-party, including the Defendants, has any ability to redirect those assets or alter the smart contract rules that control their movement.

To obtain transactional privacy using the tool, an Ethereum user sends her tokens to a Tornado Cash pool address on the Ethereum blockchain. The smart contract published at that address locks those tokens, but allows the sender to release them to a new, apparently unconnected Ethereum address at a later date. To anyone attempting to track the user's activities across the Ethereum blockchain, they will see that she moved tokens to a Tornado Cash pool address, but will not know which release from that address was under her control because it will be sent to a new address with no obvious connection to the user's earlier activities. It is helpful to think of Tornado Cash as an extension of the Ethereum protocol: Ethereum allows users to send tokens from address to address, and Tornado Cash allows users to do that with privacy. Neither Ethereum nor Tornado Cash requires users to put their trust in anyone while transacting, and neither allows any third party to control the user's assets while transacting.

Users can do all of the above with nothing but an internet-connected computer to write and broadcast a transaction message that obeys the syntactic rules of the Ethereum protocol and the Tornado Cash smart contracts. This means that Tornado Cash users can have the benefit of transactional privacy while using *only* the immutable and non-custodial smart contracts on Ethereum and no other third-party software, websites, or infrastructure. Alternatively, users can write and broadcast these transaction messages by using the Tornado Cash user interface ("UI") software. The UI can be thought of as an interactive guide to correctly authoring, signing, and broadcasting these transaction messages. As helpful as this is, the UI is still just software running on the user's computer. It was released as a fully open-source standalone software package that can be downloaded and installed on any users' computer locally, and it was also made available on-demand at a web server maintained by Amazon Web Services ("AWS") and paid for by the Defendants. In all cases, the user

is the only person who can initiate the transaction by signing the message with cryptographic keys she has stored on her computer. The UI is, in this sense, rather like an early version of Turbo Tax. It will help you fill out your tax forms by prompting you with non-technical questions, but you are ultimately responsible for printing out the results, filing them, and paying your taxes yourself.

Users also have the option of paying a third party, called a "relayer," in order to improve the privacy of their transactions. This relayer is, however, merely relaying already formed and user-signed transaction messages to the Ethereum network and paying the associated Ethereum transaction fees. To continue the tax preparation metaphor, the relayer is like a private courier server the taxpayer hires to deliver her tax documents to the IRS. At no point can a relayer alter the signature of the transaction, control the underlying funds, or otherwise manipulate the assets that the user is moving. If a relayer fails to relay the message, the user can always broadcast the transaction message herself or find an alternative relayer. The indictment alleges only that Defendants curated a list of available relayers that users might engage. The indictment does not allege that Defendants acted as relayers themselves or had any specific knowledge of specific users paying specific relayers.

To be eligible to be included in the curated relayer list, relayers were required to prove control over a certain amount of an Ethereum token called Torn on the Ethereum blockchain. Defendants are also alleged to have held Torn tokens. The only enrichment from Tornado Cash's operation that Defendants are alleged to have received is from the hypothesized increased demand for Torn tokens that is assumed to have resulted from this token-holding requirement coupled with a hypothetical resultant increase in the price of Torn on secondary markets. This is an extremely attenuated claim with no evidence offered in the indictment as support. Even if it is accurate it does not create any direct pecuniary link between any alleged users of the protocol (*e.g.* the Lazarus Group) and the Defendants. Indeed, the reputational effects from criminal usage of Tornado Cash likely decreased the value of these tokens, as the value of the privacy protocol to legitimate users decreases if risk-

averse centralized exchanges refuse to accept any tokens that have transactions traced back to a smart contract address that shows evidence of criminal usage. Contrary to the prosecution's claims of enrichment, during the relevant period the value of Torn tokens plummeted.[3]

As discussed, nobody can rewrite the Tornado Cash pool smart contracts in order to change how they work or gain control over user funds stored therein. The other software associated with the protocol is not immutable, but this software does not control user funds and is not essential to the operation of the protocol. The non-pool smart contracts, such as the relayer registry, can be upgraded and altered but such changes could never result in users losing access to their funds; nor could changing these smart contracts deny any potential users future access to the immutable pool contracts and the primary benefits of the privacy protocol generally. Nor would rewriting the off-chain UI software prevent misuse of the privacy tool by criminals. Releasing new versions of the UI would not automatically replace previously released versions of the software that may be retained by users or obtained from other third-party websites. Nor would it force users to use only the newly rewritten software: users can always use older versions of the interface or use the immutable pool contracts directly. Accordingly, the developers (1) have no control over software on the Ethereum blockchain that actually controls user funds, and (2) have no control over users' choice of any supporting software: they could publish a new version of the UI or amend the non-pool smart contracts with altered functionality, but users would be free to use previous versions of the Tornado Cash protocol with previous functionality if they so desire.

III. Alleged Activities of the Defendants

We do not have any personal knowledge of the activities of the Defendants. We do, however, have many years of experience researching and explaining the type of technology that Defendants

[3] See TORN, CoinMarketCap, perma.cc/Z6YV-WV4A (as the protocol became more popular from early 2021 to summer 2022 before OFAC's sanctions, TORN price crashed from $400 to $18).

built and released, including the Tornado Cash protocol specifically, and the manner by which software developers in the cryptocurrency space typically develop, release, and maintain such tools. Developers *publish* smart contract software to the Ethereum blockchain. Some of that smart contract software is immutable and cannot be updated after publication. Developers also *publish* user-interface and other supporting software to web servers. They may *pay* fees to maintain these web servers. A server will often both (a) *communicate* the contents of that server, the open-source software, to users of that software for their use and (b) *communicate* messages generated by users with that software back to the Ethereum peer-to-peer network. To our knowledge, this is a complete description of the activities of the Defendants. The indictment does not plainly contradict this description, but it does use vague and prejudicial language to describe these activities.

The indictment does not allege any facts indicating that the Lazarus group or any other sanctioned entity used the Tornado Cash UI software or the AWS web server hosting that UI. Generally, a sophisticated user moving large amounts of tokens would use the smart contract directly and would not use the supporting UI software or the web server. Typically, none of the data or messages communicated by a developer's web server on behalf of users will be essential to a user's operation of an ethereum smart contract. The only discretion developers will have over the communication of that user data is whether or not to communicate it. Because of digital signatures, developers typically have no power to alter the data in those communications or change the economic substance of the transaction messages communicated; they also have little actual knowledge of who is sending these messages beyond an Ethereum address and, sometimes, an IP address. Accordingly, developers cannot redirect, seize, or otherwise control any assets described by those messages. This is true for most decentralized app developers and, to our knowledge it is true of the Tornado Cash UI and its developers, the Defendants. In this sense, the AWS web server was nothing like an online banking website where the bank is technically and legally responsible for acting at the behest of its

customers, handling their money and following their direction via online interactions. Instead, the AWS web server is like an internet content delivery network: it is but one of many ways to move packets of data between, for example, a Netflix viewer and Netflix's servers. In this case the server is simply one way among many to move signed transaction messages from a Tornado Cash user's computer to the Ethereum network that ultimately executes the transactions by including them in the blockchain.

The indictment wrongly characterizes the activities of the Defendants as "execut[ing]" transactions, "provid[ing]" secret notes, "initiating" transfers, "commingl[ing]" deposits, and "receiving" funds.[4] To our knowledge and based on the allegations in the indictment, the Defendants did not execute any user transactions, provide any secret notes, initiate any user transfers, commingle any user deposits, or receive any user funds. The Defendants *did* create and publish open-source software that allowed individual users to do many of these things on their own: They published immutable and non-custodial smart contracts that ultimately "receive" user funds, allowing the users and only those same users to take them back on demand. But to say that they receive those funds is like saying a locksmith owns everything secured by his locks. They published software that allows users to generate secret notes and transaction messages that can be signed by the user and executed by the Ethereum network. They paid AWS to host that open-source software on websites powered by U.S. corporations in order to make it easier for the public to find and use that software. To our knowledge and as alleged in the indictment, they did *not* take any fees in return for the usage of the AWS web servers or their open-source software.

As described in the indictment, when alerted to the Lazarus Group's usage of their software to launder hacking proceeds, the Defendants voluntarily implemented screening on their website to

[4] Indictment (Doc. 1) ¶¶1, 9-31.

discourage its usage by known bad actors. Alluding to their failure to change immutable software on the Ethereum blockchain (an impossibility) the indictment wrongly suggests that the Defendants "took no action to prevent the Tornado Cash service from facilitating this money laundering."[5] Indeed, they took action in the only way that was possible: they voluntarily blocked known persons from accessing the web server where some versions of the software were hosted. Given the immutability of the Ethereum blockchain and the widespread distribution of open-source software, there was, to our knowledge, no other effective action that could be taken. Even the best corporate citizen can't unrelease and make disappear open-source software that's already been widely distributed. All one can do is try to stop criminals from downloading a new copy of that software from one's servers. Similarly, even the most powerful attorney cannot force the recipient of a misdirected email to destroy it and forget about its contents; once information is widely released it is effectively impossible to stop certain people from finding and using it.

The indictment disparagingly refers to the Defendants as "[c]laiming to offer the Tornado Cash service as a 'privacy' service, [when] the Defendants in fact knew that it was a haven for criminals."[6] Respectfully, there are several problems with this characterization. First, Tornado Cash is not a service in the traditional sense of the word. Like Ethereum, it is a series of open-source software tools that can be used without any involvement from any third-party service provider. Second, it is a freely available privacy tool and, like any other widely available tool, it will provide its functionality for anyone who wields it—be they a criminal or a law-abiding citizen. Criminals use cars to evade law enforcement and yet we do not suggest that cars are not legitimate tools for transportation because they are, instead, a haven for criminals. Coin Center has used Tornado Cash to privately accept donations that support our non-profit mission. We have brought a lawsuit to have OFAC remove the

[5] Doc. 1 ¶66.
[6] Doc. 1 ¶1.

Tornado Cash pool addresses from the sanctions list so that we can continue to use them for that purpose and so that other Americans can use them for any legitimate privacy purposes.[7] We have co-plaintiffs in that lawsuit who wish to use Tornado Cash to be privately paid their salary and who have used it to privately make donations to the war effort in Ukraine without becoming targets of Russian cyber attacks.[8]

Nor is Tornado Cash the only tool of its kind. JP Morgan Chase previously built and tested a computer system, called "Quorum," for privately settling accounts between banks using the very same zero-knowledge proof cryptography as Tornado Cash. Recently, it has been reported that they are testing a similar zero-knowledge system that, like Tornado Cash, runs on the Ethereum network, called "Aztec." These tools are widely regarded by top researchers in cryptography[9] and finance[10] as state-of-the-art and essential for providing privacy safeguards when using blockchains to transact. To suggest that Tornado Cash is a mere haven for criminals rather than a series of innovative privacy tools for the world is inaccurate and inflammatory. There are larger public policy discussions worth having regarding the costs and benefits of online privacy tools but this is not the appropriate forum for that debate. The prosecution is not even attempting to have that debate, choosing instead to incorrectly pigeon hole a widely used and valuable new invention as a mere "haven for criminals."

---

[7] *See Coin Center v. Yellen*, 2023 WL 7121095 (N.D. Fla. Oct. 30).
[8] *Id.*
[9] *See* Miers, et al., *Zerocoin: Anonymous Distributed E-cash from Bitcoin*, Proceedings of IEEE Symposium Security and Privacy, at 397–411 (2013) ("Decentralized currencies should ensure a user's privacy from his peers when conducting legitimate financial transactions. Zerocash [a progenitor of Tornado Cash] provides such privacy protection, by hiding user identities, transaction amounts, and account balances from public view.").
[10] *See, e.g.,* Nadler & Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, Fed. Reserve Bank of St. Louis Rev., at 122-136 (2023) ("We conclude that non-custodial crypto asset mixers are an interesting innovation and demonstrate the power of zero knowledge proofs. They provide honest users with the option not to share their transaction history publicly and use public blockchains similarly to other electronic payment systems.").

Another key descriptive error made by the prosecution is the repeated use of the word "customer" to describe users of the tool.[11] Again, the tool is not a service provided by a business, it is a series of open-source software tools that anyone is free to use. We refer to the people who use this tool as "users," and that is the common and widely accepted term for such persons in the larger open-source software ecosystem. People use open-source software all the time without becoming customers of the software developer in any way, shape, or form. For example, if one visits almost any website, one is likely to be using open-source software libraries that store, relay, encode, and decode the relevant text and images. One is not a customer of Wikipedia by virtue of reading an article found at wikipedia.org. This statement remains true even though the Wikimedia Foundation, like the Defendants, pays a series of US companies to host that open-source software and make available its content to the public. The foundation may be a customer of Amazon for cloud storage services but that certainly does not make an intrepid fifth grade student into a customer of Wikipedia when she uses the site to do her history research. She is a user of Wikipedia and a user of the open-source software that powers that website. She is not a customer. The fact that fees must be paid to use the Tornado Cash protocol may facially erode the validity of that comparison, but as we have described throughout, no fees are ever paid to the developers of the Tornado Cash protocol. Those fees that are typically paid by users are either Ethereum transactions fees (fees that are inherent in any use of Ethereum for any purpose) or relayer fees (fees optionally paid to a third party to broadcast private transaction messages). These fees are no more relevant to the Tornado Cash developers than your payment for gasoline is relevant to the manufacturer of your car.

With a firmer grasp on the actual mechanism by which the Tornado Cash tool operated and a better understanding of the actions of the Defendants, we will now briefly turn to a discussion of

[11] *E.g.*, Doc. 1 ¶10.

whether these actions could possibly rise to the level of culpability for the charged sanctions offenses. Other Amici have effectively addressed the unlicensed money transmission[12] and money laundering charges,[13] so we will deal only with the sanctions evasion charge.

IV. Sanctions Laws and Decentralized Protocols

Sanctions laws at their core allow the President to block and prohibit *transactions*.[14] The factual allegations against the Defendants are limited to publishing open-source software and paying for web servers that communicate information related to that open-source software. Many of these activities are not transactional at all, *e.g.* publishing open-source software without any fee or license requirement for users, or communicating user-signed transaction messages without taking any fees. Those activities that arguably are transactional, *e.g.* paying for a web server that hosts open-source software, are statutorily exempted transactions to which sanctions prohibitions cannot apply. Accordingly, none of the alleged actions taken by Defendants are transactions that can be prohibited under U.S. sanctions laws.

Congress, concerned with the potential for sanctions laws to chill speech and free trade in ideas, passed two laws that exempt transactions in information from the prohibition powers in IEEPA. In 1988, Congress passed legislation that withdrew from the executive any "authority to regulate or prohibit, directly or indirectly, the importation from any country, or the exportation to any country, whether commercial or otherwise … of publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, or other informational materials."[15] This change to sanctions laws came to be known as the Berman Amendments, after its lead author. Later, in response to a series of cases where the executive attempted to narrowly interpret the Berman Amendments

[12] *See* Amicus Br. of Blockchain Ass'n.
[13] *See* Doc. 39 (Amicus Br. of DeFi Education Fund) at 17-20.
[14] See 50 U.S.C. § 1702(a).
[15] 50 U.S.C. § 1702(b)(3).

such that they would no longer protect informational materials in novel formats, including software, Congress passed further legislation, the "Free Trade in Ideas Act," which explicitly expanded the class of exempted transactions to "any information or informational materials."[16]

These broad statutory exemptions have since been incorporated into the promulgated regulations.[17] The regulations also include a carve-out from the statutory exemptions that effectively reapplies prohibitions to certain types of information transactions when the information is to be created on-demand, *after* the transaction.[18] Arguably this regulation goes against the plain meaning of the statutory carve-out "any information or informational materials." Irrespective of the legality of the executive's narrowing of the statutory carve-out, all of the information materials related to the Defendant's transactions were "fully created and in existence at the date of the transactions."[19] The indictment does not allege any transactions for custom-made information products to any sanctioned persons for delivery after some payment, as is found in the very few cases where an information transaction was lawfully sanctioned.[20]

---

[16] 108 Stat. 382, 474-75 (1994); 50 U.S.C. § 1702(b)(3); *see* Taylor III, *Information Wants to Be Free (of Sanctions): Why the President Cannot Prohibit Foreign Access to Social Media Under U.S. Export Regulations*, 54 Wm. & Mary L. Rev. 297, 308 (2012) ("Congress positioned FTIA in such a way as a response to OFAC's attempts to narrowly interpret the Berman Amendment, for example by limiting 'the type of information that is protected or ... the medium or method of transmitting the information.'") (quoting H.R. Rep. No. 103-482, at 239 (1994)).

[17] *See* 31 C.F.R. § 560.210(c)(1) ("The prohibitions contained in this part do not apply to the importation from any country and the exportation to any country of information or informational materials, as defined in § 560.315, whether commercial or otherwise, regardless of format or medium of transmission.")

[18] *See id.* § 560.210(c)(2) ("This section does not exempt from regulation or authorize transactions related to information or informational materials not fully created and in existence at the date of the transactions, or to the substantive or artistic alteration or enhancement of informational materials, or to the provision of marketing and business consulting services.")

[19] *Id.*

[20] *See, e.g.*, *United States v. Griffith*, 515 F. Supp. 3d 106, 117 (S.D.N.Y. 2021) ("The government has represented, both in their brief and at oral argument, that Griffith's speaking engagement at the April 2019 conference was a major step in a long-term plan to persuade and assist the DPRK in using Ethereum to avoid sanctions and launder money."); *United States v. Amirnazmi*, 645 F.3d 564, 587-88 (3d Cir. 2011) ("At trial, the government adduced sufficient evidence to convince a reasonable

The prosecution may argue that it is not charging Defendants with violation of IEEPA but rather with conspiracy to violate IEEPA, that even if the Defendants did not engage in prohibited transactions, their publication of software used by others to engage in sanctioned transactions is sufficient to show agreement and intent to violate the law. First, the Berman Amendments do not cabin their safe harbor so narrowly, they removed from the executive any power to "*directly or indirectly*" prohibit information transactions.[21] If one can be charged with conspiracy to violate sanctions merely for engaging in information transactions, that is an "indirect" prohibition on those information transactions. Similarly, if it is lawful under the Berman Amendments to develop and publish software, then it is lawful to *agree* and *take substantial steps* to develop and publish software.

Second, all of the most consequential steps taken by the Defendants to make available the Tornado Cash protocol, *i.e.* publishing the immutable pool smart contracts to the Ethereum blockchain, took place long before the Lazarus Group hacked the Ronan bridge and long before there was any indication that any sanctioned persons would be using the protocol. Publishing decisions over the functionality of the software and how to release it were made long before any knowledge of the Lazarus Group's activities could have even existed. After April 14th, the Defendants, as alleged, took a single day to decide to block traffic associated with identified Lazarus Group wallets from using their web server, the only part of the Tornado Cash protocol under their control. That they failed to retract previously released software or change the immutable pool contracts, an impossibility given the Ethereum blockchain's operation, in no way suggests that they willfully and knowingly confederated to commit sanctions evasion. To argue to the contrary would be to suggest that the developers of the Linux open-source operating system confederated with the regime of Iran, merely by freely releasing

---

factfinder beyond a reasonable doubt that ChemPlan [software] was not 'fully created and in existence' at the date of the relevant transactions. Amirnazmi trumpeted the software's dynamism.").

[21] 50 U.S.C. § 1702(b) (emphasis added).

a valuable computing tool that Iran would later use to operate computers related to its weapons programs. Crafting such a broad standard for sanctions liability would massively chill the publication of software and could be used to villainize countless researchers, scientists, and developers whose selfless release of free and open-source software is largely responsible for the information technology revolution of the last half-century.

Nor are the Defendants alone in claiming such exempted transactions from sanctions laws. Aside from several litigated cases,[22] it is worth noting that even traditional global financial technology providers claim exemption on the basis of merely providing information transactions. For example, The Society for Worldwide Interbank Financial Telecommunication, SWIFT, is a Belgian banking cooperative that helps banks across the world settle over $150 trillion in financial transactions a year.[23] While SWIFT's tools are often used to move substantial amounts of money in violation of sanctions, and while SWIFT voluntarily cooperates with ongoing investigations into the use of their messaging protocol for sanctions evasion,[24] they are, nonetheless, at pains to stress that they are *not* an obligated entity under sanctions laws:

> Responsibility for ensuring that individual financial transactions comply with sanctions laws … rests with the financial institutions handling them, and their competent authorities. Swift is only a ***messaging service provider*** and has no involvement in or control over the underlying financial transactions that are mentioned by its financial institutional customers in their messages.[25]

SWIFT has, in fact, far more control over the messages that they relay than the Tornado Cash developers have over any Tornado Cash messages. Unlike the Tornado Cash protocol, SWIFT

---

[22] *See Cernuda v. Heavey*, 720 F. Supp. 1544 (S.D. Fla. 1989); *Kalantari v. Nitv, Inc.*, 352 F.3d 1202 (9th Cir. 2003).

[23] *SWIFT Plots Real-Time Role for Next 50 Years of Cross-Border Payments*, PYMNTS (Oct. 3, 2022), perma.cc/KL2G-7VAX.

[24] *See e.g.* Parsons, *What You Need To Know About Swift and Economic Sanctions*, Johns Hopkins U. (Mar. 2, 2022), perma.cc/2T2R-FLFE.

[25] *Compliance: Swift and Sanctions*, Swift, perma.cc/6TM2-MZDX (emphasis added)

messages can be relayed only by SWIFT-authorized users and SWIFT can and does block some users from participating in their proprietary messaging network.[26]

As discussed, Tornado Cash uses the open Ethereum network for message communications and Tornado Cash software developers have no ability to restrict access to that network and no ability to remove or alter the functioning of the Tornado Cash pool contracts that hold user funds. Some Tornado Cash messages may be communicated by the AWS web server paid for by the Defendants, but these services are neither necessary nor sufficient for usage of the Tornado Cash protocol. Messages can also be communicated by the user herself directly to the Ethereum blockchain or by third-parties such as relayers. Further, the indictment does not clearly allege that sanctioned persons even utilized the AWS server. And, as alleged in the indictment, the Defendants quickly took all available steps to block newly announced sanctioned persons from accessing that web server in the future.

Like the Defendants, SWIFT has voluntarily taken actions to assist law enforcement in investigating and preventing sanctions evasion after evidence of illicit usage has come to light. Unlike the Defendants, SWIFT wholly controls the messaging infrastructure that moves user funds; unlike the Defendants, SWIFT could but has chosen not to block all messages dealing with blocked property or sanctioned persons. Fortunately for Defendants (as well as SWIFT), IEEPA correctly forbids the President from directly or indirectly (as here with a conspiracy charge) prohibiting mere transactions in information.

[26] See *Corporate Rules*, Swift (Nov. 7, 2023), *available at* perma.cc/6VSU-F8AX.

V. First Amendment Defenses

The Berman Amendments were intended to shield First-Amendment-protected activities from the reach of IEEPA's prohibitions.[27] Should these statutory exemptions fail to protect the Defendants from liability, the First Amendment also protects them. At root, the prosecution is attempting to hold the Defendants liable for the content and viewpoint of their speech. The software published and released by the Defendants carries a deep political and cultural message concerning both (a) whether people should be able to make private peer-to-peer financial transactions online and (b) exactly how and by using which scientific and cryptographic principles they can make those transactions.[28] The software does not make those transactions for them nor do the Defendants. The software is an interactive guide and a body of research that has been distilled into a free and open-source package that others can read, learn from, and choose to use. Defendants' choice regarding how to write and publish the software is the expression of a powerful political and scientific viewpoint in and of itself. Some in the U.S. Government may strongly have preferred that they would have published their code with a secret vulnerability or a "backdoor" for law enforcement, or simply not published their viewpoints at all. Especially in light of that probable government bias, the Defendants cannot and should not be held liable for having merely published software as they saw fit.[29]

---

[27] *See Cernuda*, 720 F. Supp. at 1553 ("the court holds that statutory construction and the legislative history of the 1988 TWEA amendment show that Congress amended the TWEA to exempt 'informational materials,' in order to prevent the statute from running afoul of the First Amendment.").

[28] *See generally,* Brito, *The Case for Electronic Cash 1.0* (Feb. 2019), perma.cc/PP78-Q3L2 ("For close to a decade, cryptographers and computer scientists have been working to improve on Bitcoin's design in order to build a cryptocurrency that is not only permissionless and censorship-resistant, as Bitcoin is, but also private. … Caring deeply about the freedom that [electronic] cash engenders is part and parcel of the Western liberal tradition.").

[29] *See 303 Creative v. Elenis*, 143 S. Ct. 2298, 2303 (2023) ("the First Amendment protects an individual's right to speak his mind regardless of whether the government considers his speech sensible and well intentioned or deeply misguided, and likely to cause anguish or incalculable grief") (cleaned up).

In *IMS Health v. Sorrell*, the Supreme Court held that a ban on the sale of prescriber identifying information by-and-to marketing professionals and data brokers was an unconstitutional speaker- and content-based burden on protected expression.[30] The Court said that it was unnecessary to determine whether the data being bought and sold was protected speech or merely a valuable commodity; it was enough that the law burdened the expressive activities of marketers and data brokers.[31] Unlike IMS Health, Defendants were not buying or selling any information related to the Tornado Cash app. They simply made a software tool available for the creation of information (the Ethereum transaction messages) by its users and, at most, communicated some of this information for those users *gratis* via the AWS web server. Nonetheless, the prosecution has targeted Defendants for severe criminal penalties exclusively because of the content of their publications and the viewpoints expressed therein.

Even if the Defendants had been taking fees for usage of their software or the AWS web server, their activities would still be strongly protected by the First Amendment. In *303 Creative LLC v. Elenis*, the Court articulated a highly protective standard for web developer speech even in the context of for-profit publishing.[32] The Court held that it would be unconstitutional "to forc[e a web developer] to create custom websites" for profit.[33] The Court explained that the act of publishing websites containing "images, words, symbols, and other modes of expression" was protected as "pure speech" and not as expressive conduct.[34] The Court explicitly rejected the premise, argued by the government, that the regulation was focused merely on *selling* web development services, or some

---

[30] *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011).
[31] *Id.* at 571. The Court reasoned that the law in question "could be compared with a law prohibiting trade magazines from purchasing or using ink. Like that hypothetical law, [the law in question] imposes a speaker- and content-based burden on protected expression, and that circumstance is sufficient to justify application of heightened scrutiny. As a consequence, this case can be resolved even assuming, as the State argues, that prescriber-identifying information is a mere commodity." *Id.* (cleaned up).
[32] *303 Creative*, 143 S. Ct. 2298.
[33] *Id.* at 2313.
[34] *Id.* at 2312.

other form of regulatable commercial conduct.[35] Accordingly, the Court subjected the regulation in question to strict scrutiny and found that it was not narrowly tailored to serve a compelling government interest.

Because of the Berman Amendments, IEEPA cannot create criminal liability for merely publishing software and websites. If IEEPA did create such liability, then it would, per *303 Creative*, directly prohibit certain forms of "pure speech," and, per *IMS Health*, directly burden speech based on the viewpoints of publishers. The law would have to overcome strict scrutiny, which it cannot. Finally, the rules of lenity and constitutional avoidance counsel that any doubts that the Court has about these questions should be resolved in favor of the Defendants.[36]

CONCLUSION

This Court should hold that the Berman Amendments do not allow criminal liability for transactions in information, including under a conspiracy charge. Alternatively, this Court should hold that any such criminal liability would violate the First Amendment.

Dated: April 5, 2024

Respectfully submitted,

/s/ Daniel M. Vitagliano

Peter Van Valkenburgh*
Coin Center
700 K St. NW
Washington, D.C. 20001
peter@coincenter.org

**pro hac vice applications forthcoming*

Cameron T. Norris*
Daniel M. Vitagliano (SDNY 5856703)**
Jeffrey S. Hetzel*
Consovoy McCarthy PLLC
1600 Wilson Boulevard, Suite 700
Arlington, Virginia 22209
(703) 243-9423
dvitagliano@consovoymccarthy.com

*** supervised by principals of the firm admitted to practice in Virginia*

[35] *Id.* at 2319.

[36] *See United States v. Dauray*, 215 F.3d 257, 264 (2d Cir. 2000) ("'In criminal prosecutions the rule of lenity requires that ambiguities in the statute be resolved in the defendant's favor.'"); *FEC v. Pol. Contributions Data, Inc.*, 943 F.2d 190, 191 (2d Cir. 1991) ("we are obliged to construe statutes to avoid constitutional problems whenever possible").